PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

#3

Helsinki 24.3.2000

4

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	**IntraSecure Networks Oy** **Espoo**
Patenttihakemus nro Patent application no	**990265**
Tekemispäivä Filing date	**10.02.1999**
Kansainvälinen luokka International class	**H04L**
Keksinnön nimitys Title of invention	

"Data communication method for sending a message trough a firewall"
(Tietoliikennemenetelmä viestin lähettämiseksi palomuurin läpi)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu	300,-	mk
Fee	300,-	FIM

DATA COMMUNICATION METHOD FOR SENDING A MESSAGE THROUGH A FIREWALL

TECHNICAL FIELD

The invention is concerned with a data communication method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall. The method can be used for sending protected messages with various kinds of protection methods, computer networks and network protocols and is expected to be very useful for instance for sending secret messages.

DESCRIPTION OF RELATED ART

A computer network is formed when two or more computers are connected to each other. Local area networks (or internal networks) may be formed of the computers within a company, while wide area networks may be extended over bigger areas, such as many towns and even countries. The networks may be connected via cables, fibers and/or radio links.

An example of a global network is the Internet. This worldwide network can be used for communication, delivering and searching for information.

If an internal system for electronic post is installed, everyone connected to the local network can send messages to each other. The local network can be connected to another network, which can be an external network, such as Internet, and so electronic mail can be sent to the whole world to everyone connected to the external network. Internet is the most common network for data communication, by for example E-mail.

The fact that several local networks can be connected to other networks, Internet in particular, sets up requirements for the security and the equipment therefor.

There are different systems for the improving of the security. It is important that data within an internal network is protected so that only right users can change and read it. The users usually identify themselves with a user name and a password. Also other security details exist. Other security problems are network errors and work stops. With increasing complexity, advanced security systems become important.

The popularity of Internet can be seen on the fact that new network products and services are developed all the time. These products are developed in accordance with new Internet standards and are applied to the protocols used in transfers on Internet.

A firewall is a security system to protect a network against infringement from unauthorized users in other networks, such as Internet. A firewall can hinder computers from communicating directly with other networks, such as external networks, and vice versa. Instead, all communication is sent through the firewall placed outside the internal network. The firewall decides if it is safe to let messages and files pass between the external and the internal network on the basis of the addresses of the message, that can be in form of data packets, and different parameters. The firewall thus controls the communication between the internal and external network and modifies the data packets of for example TCP/IP based Internet (with respect to the TCP/IP protocol, see the next page). Usually, a firewall translates network addresses and other data defining the communication so that the internal address and the internal parameters are changed to an external address and external parameters. This means that for instance IP addresses used in an internal or local network are hidden from outside users. A packet coming from an external network to an internal network is modified back by the firewall.

The firewall can be formed in many different ways and is usually designed individually from case to case in accordance with the actual needs of the network. If the amount of traffic through the firewall is very high, quite extensive hardware for the firewall computer is needed.

Another method of increasing the security is by means of protection of the messages to be sent by for instance tunneling in virtual networks. In virtual networks several local and global networks use Internet to be connected to each other. By tunneling, data is transferred between two networks via a third network, such as Internet. In this technique, a given kind of data packets of a given protocol is encapsulated in packets of another protocol. Packet mode is a transfer method that can be used in virtual connections. In this technique data is sent in small "packets" with an address and a sender, so that several persons can use the connection simultaneously. The other protocol is usually TCP/IP, when the transfers go through Internet. The own protocols are packed in the TCP/IP packages that are sent via Internet.

The data communication between computers is carried out according to given rules which are called protocols. TCP/IP is one such protocol and is an abbreviation for Transmission Control Protocol/Internet Protocol. Standards for TCP/IP are well documented in so called RFC (Request for comments) documents. The IP protocol takes care of the data packets and is responsible for that the packets find right addresses. The data packets are addressed by means of internet addresses and go from computer to computer until the right destination is reached. Communication with IP is connectionless as no fixed connection exist between communicating computers. The message is going forward step by step. The TCP protocol takes care of the transferring of messages between two computers by making a virtual connection between them without any physical connection. The TCP is the transport protocol that is responsible for the connection itself between sender and receiver. Also other standards than TCP/IP can be used in Internet.

The packets go through the "tunnel" maintained by Internet to the receiver, where the packets of different protocols are separated from each other and return to the original form. The authorization of the receiver can be controlled in different ways. The authorization control can be carried out in two steps: authentication and authorization. Authentication is carried out to control the identity of the user, while the authorization defines what the user is authorized to do.

The virtual networks give a high security. The secret information has an own channel on Internet as a result of different methods of authentication, encryption and/or encapsulation.

The security of Internet is not sufficient for all types of transfers. There are however ways to protect e-mail and other messages sent through internet from others. Especially high security can be achieved by encryption.

Encryption means that messages are changed before sending so that they cannot be read before decryption with a special key and usually also by confirming that the right person sent the message (authentication). There are a big variety of encryption methods of the above kind.

In many protection methods all connections have different parameters. The function wherein the real protection is made is called transformation. In the transformation function the packet is changed in accordance with given parameters depending on the actual protection used.

One problem with firewalls is the need of extensive equipment for the firewall computer if the traffic amount of traffic through the firewall is high.

Another problem with firewalls is that if protection methods are used and the network is protected with a firewall, the firewall cannot identify the messages to be sent and will therefore not let them pass.

In existing methods, the protection function or the parameters for the protection are given to the firewall so that the firewall can identify or protect the message and the message can then be sent through the firewall. The drawback with such methods is decreased security for the local network as secret information is delivered outside the local network.

US patent 0715668 is mentioned as such prior art. The patent is about secure transfer of information between firewalls over an unprotected network. Internet protocol security and IPSec messages are handled in the firewall without assuming that encrypted messages has access to all services by decrypting the message and controlling the access.

Another such method is described in US patent 0586231, wherein a firewall computer is allowed to provide virtual tunnel records and secret keys.

In the European patent application EP 0 858 201 an electronic data transfer system transmits a message between the first computer system, arranged within a firewall, and a second computer system. Messages that are not suitable for transmission through a firewall are translated in a format that is appropriate for transmission across the firewall.

THE OBJECT OF THE INVENTION

An object of the invention is a method of sending messages that decreases the work to be done by the firewall computer compared with previously known methods.

The second object of the invention is a safer method of sending protected messages through a firewall.

More in detail, the second object of the invention is a method wherein protected messages can be sent through a firewall without delivering information about the parameters of the protection outside the local network to the firewall.

DESCRIPTION OF THE INVENTION

In the method of the invention a message is sent on a computer network from a first computer system to at least one other computer system through a firewall. In step a), a request with data for a new connection between the first computer system and at least one other computer system is sent from the first computer system to the firewall. In step b), up on approval of the message, information about the necessary modifications to be made in a message that is sent via the requested connection through the firewall is sent from the firewall to the first computer system. In step c), the message to be sent is modified in the first computer system in accordance with the information sent from the firewall. In step d), which is optional and can be carried out before step c) or after step c), identification data of the connection for the message to be sent between said computer systems is sent to the firewall so that the message can be identified by the firewall to be able to pass the same. In step e), the message is then sent from the first computer system to the at least one other computer system through the firewall.

In an application of the method, the message to be sent is protected as the method is very suitable for sending protected messages. The message to be sent between said computer systems is in that case protected in step c) after it has been modified, whereby step d) is necessary and the data to be sent from the first computer system to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

The protection method can be some method known in the art. One suitable way to protect the message is to use methods defined in the standard RFC 1825 for TCP/IP. This standard includes sub standards for for instance authentication methods and encryption methods, which can be used separately or simultaneously in a message sent with the method of the invention. RFC 1825 is a standard defining the IPSec security system standard, which consists of technology principles for the method used. IPSec, in turn, has sub standards for encryption, such as ESP, which is an abbreviation for encapsulated security protocol and AH, which is an abbreviation for a standard in IP for authentication. The authentication method might be MD5, SHA or other method known in the art. The encryption method might be some known method such as DES, Blowfish or the like.

In step a), the request for a new communication sent from the first computer system to the firewall contains for instance data of the new connection to be opened between the first computer system and at least one other computer system in for example in form of address identification data and such other parameters. Typical other parameters are for instance IP Data (the sender address, the receiver address), the type of protocol and TCP data: the sender port and the receiver port. The port defines the application for sending the data with e.g. TCP/IP, such as the program used, the web browser etc.

In step b), typical parameters that the firewall modifies so that the messages can pass through are the above data, for instance IP Data (the sender address, the receiver address), the type of protocol and TCP data: the sender port and the receiver port. The modifications might comprise all data of step a) or a part of them. All of the data to be modified might be known by the firewall even if not exactly included in step a).

Messages can only go through a firewall if the firewall can identify them to be allowable messages. In step d), identification data for the protection used to protect the message to be sent between said computer systems is sent to the firewall so that the protected message can be identified by the firewall. The identification data is in such a form that the firewall can identify the actual connection but not the actual parameters that have been used to protect the message if the message is protected. There exist many allowed connections with the same IP address but different other parameters. The actual protected message is sent in accordance with the parameters of one of the allowed connections and shall be identified by the firewall as being allowed and safe to deliver. If the message is not protected, step d) might be unnecessary in some embodiments, but is still advantageous to carry out in other embodiments, for instance if much traffic is going through the firewall, step d) might speed up the sending.

In the invention, the inventive idea is that a part of the firewall functionality has been given to another computer function and is carried out in the first computer system. If the message is protected, the firewall and the first computer system transfers necessary information so that the firewall would be able to pass the protected messages without having knowledge about the actual parameters used to protect the message to be sent.

In the following, the invention is described by means of some preferred embodiments of the invention. The details of the embodiments can vary within the scope of the claims.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a flow sheet over the different steps of the method of invention

Figure 2 is a schematic view of the computer network within which the data communication of the invention is carried out

DETAILED DESCRIPTION OF THE INVENTION

Figure 2 is a schematic view of a computer network within which the data communication of the invention can be carried out. A message shall be sent from a first computer system C1 to a second computer system C2.
In figure 2, the first computer system belongs to an internal network. The internal network is protected by a firewall, so that all messages to be sent and received through the firewall has to be identified and accepted by the firewall. The firewall controls data of the connection via which the messages are sent and if the connection is accepted by the firewall, the messages can pass the firewall. Before the messages can pass the firewall, they are modified in the firewall in accordance with given parameters, such as address changes and protocol changes. The computer system C1 has a virtual connection to computer system C2, which means that messages to be sent from the first computer system C1 to the second computer system C2 are sent via one or more other networks, such as external networks, for instance Internet, after having passed the firewall before ending up at and received by the second computer system C2.

Figure 1 is a flow sheet over the different steps of an embodiment of the method of the invention. A message shall be sent on a computer network from the first computer system C1 to a second computer system C2 through a firewall, which is placed outside the internal or local network to which the first computer system C1 belongs. The method of the invention can be used both for the purpose to decrease the work to be carried out by the firewall and/or for sending protected messages. If the message to be sent shall be protected before sending in accordance with the second embodiment of the invention, it can not be sent through the firewall in the normal way, because the firewall is not able to control address identification data of protected messages or forward encrypted messages. Therefor, in accordance with step a) of the invention, an information message is sent from the first computer system C1 to the firewall containing data about a new connection between the first computer system C1 and a second computer system C2 system in form of for instance address identification data, and possible other parameters for the message to be sent between said computer systems. If the firewall accepts this connection, the sending proceeds so that according to step b), information about necessary changes to be made in the message is sent from the firewall to the first computer system C1 so that the message can be sent through the firewall. The message that is intended to be protected with some protection method, that can be an authentication method and/or encryption method and shall be sent is according to step c) first modified by the first computer system C1 in accordance with the information sent from the firewall before protection. Before the protected message is sent, identification data of the protection method that have been used for protection of the message is according to point d) sent from the first computer system C1 to the firewall F so that the protected message can be identified but not read by the firewall to be able to be passed by the same. If the message is not protected, step d) is optional if the firewall used is able to identify the message. Step d) can also be carried out before step c). The protected message is then according to step e) sent from the first computer system C1 to the other computer system C2 through the firewall.

Claims

1. Method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall, characterized in the following steps:

a) sending from the first computer system to the firewall, a request with data for a new connection between the first computer system and at least one other computer system for a message to be sent between said computer systems,

b) up on approval of the connection by the firewall, sending from the firewall to the first computer system, information about the necessary modifications to be made in a message that is sent via the requested connection through the firewall,

c) modifying, in the first computer system, the message to be sent in accordance with the information sent from the firewall,

d) optionally, and before or after step c), sending from the first computer system to the firewall identification data of the connection for the message to be sent between said computer systems so that the connection for the message can be identified by the firewall and the message can pass the firewall,

e) sending the message from the first computer system to the at least one other computer system through the firewall.

2. Method of claim 1, characterized in that, the message to be sent between said computer systems is protected in step c) after it has been modified, whereby step d) is necessary and the data to be sent from the first computer system to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

3. Method of claim 2, characterized in that the protection is made using the IP Sec standard.

4. Method of claim 2 or 3, characterized in that the message to be sent is authenticated.

5. Method of any of claims 2 – 4, characterized in that the message to be sent is encrypted.

6. Method of any of claims 1 – 5, characterized in that the information message in point a) contains data of the new connection to be opened between the first computer system and at least one other computer system in form of address identification data and possible other parameters.

7. Method of claim 6, characterized in that the possible other parameters are data about the port and the protocol used for sending.

8. Method of any of claims 1 - 7 , characterized in that in step b) the modifications include address identification data and/or the port and or the protocol used for sending.

9. Method of any of claim 1 – 7, characterized in that, the message is using the TCP/IP protocol.

10. Method of any of claim 1 – 8, characterized in that, the message is sent via internet.

(57) Abstract

The invention is concerned with a method for sending a message on a computer network from a first computer system to at least one other computer system through a firewall. The method comprises the following steps: A request with data for a new connection between the first computer system and at least one other computer system is sent from the first computer system to the firewall for a message to be sent between said computer systems. Up on approval of the connection by the firewall, information about necessary modifications to be made in a message that is sent via the requested connection through the firewall is sent from the firewall to the first computer system. The message to be sent is modified in the first computer system in accordance with the information sent from the firewall. Optionally, and before or after the foregoing step, identification data of the connection for the message to be sent between said computer systems is sent from the first computer system to the firewall so that the connection for the message can be identified by the firewall and the message can pass the firewall. The message is sent from the first computer system to the at least one other computer system through the firewall. The message to be sent between said computer systems can be protected after it has been modified, whereby the data to be sent from the first computer system to the firewall includes the necessary information so that the connection for the message can be identified by the firewall.

(Fig. 1)

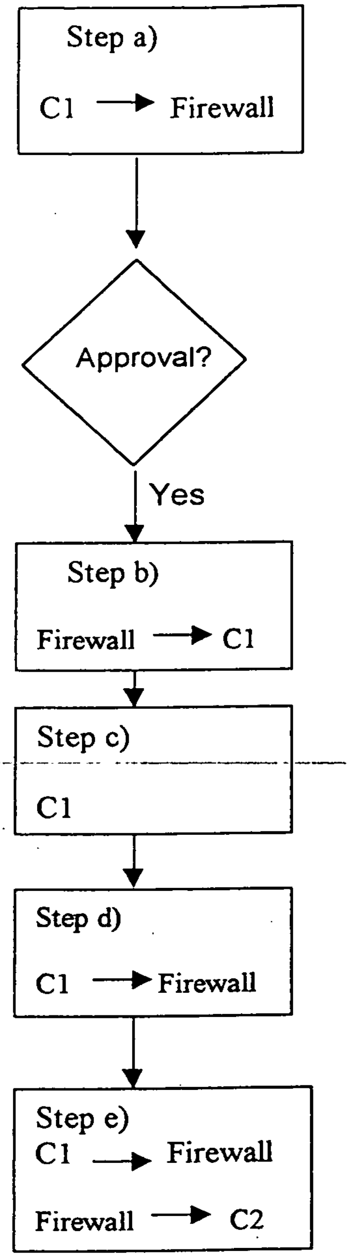
Step a)
C1 → Firewall
Approval?
Yes
Step b)
Firewall → C1
Step c)
C1
Step d)
C1 → Firewall
Step e)
C1 → Firewall
Firewall → C2

FIG. 1

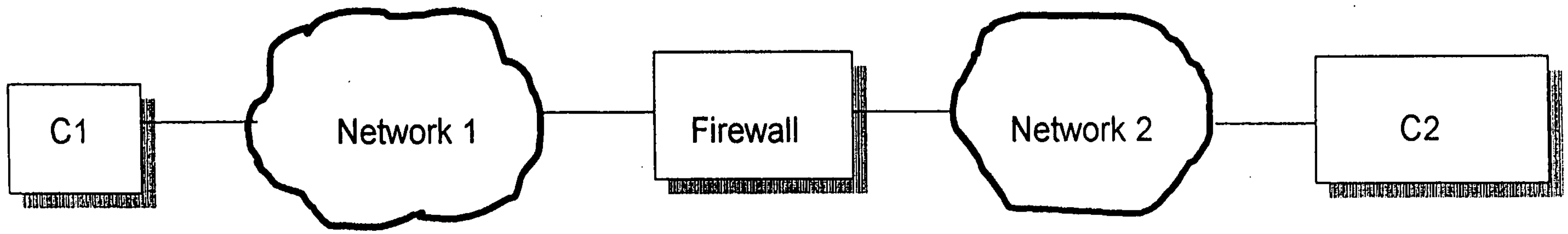

FIG. 2